Copy

PATENT

09/738571

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Sheueling Chang

Assignee: Sun Microsystems, Inc.

Title: METHOD FOR EFFICIENT COMPUTATION OF POINT DOUBLING OPERATION OF ELLIPTIC CURVE POINT SCALAR MULTIPLICATION OVER FINITE FIELDS F(2M)

Patent No.: 6,826,586 Issued: November 30, 2004

Atty. Docket No.: 004-5182

Feburary 1, 2005

ATTN: Certificate of Correction Branch
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

REQUEST FOR CERTIFICATE OF CORRECTION OF PATENT – PTO MISTAKE (37 C.F.R. § 1.322(a))

Dear Sir:

Pursuant to 35 U.S.C. § 254 and 37 C.F.R. § 1.322(a), please issue a Certificate of Correction in the above-identified matter. The mistake(s) to be corrected was made by the Office.

1. Attached hereto is Form PTO/SB/44 (PTO-1050) suitable for printing.

2. The exact page(s) and line number(s) where the error(s) is shown correctly in the application file:

   Page 15, line 5;

   Claim 13; and

   Claim 17.

3. Please send the Certificate to:

   Steven R. Gilliam
   ZAGORIN, O'BRIEN & GRAHAM, L.L.P.
   7600B N. CAPITAL OF TEXAS HWY, SUITE 350
   AUSTIN, TEXAS 78731-1191

FEB 15 2005

Respectfully submitted,

Steven R. Gilliam, Reg. No. 51,734
Attorney for Applicant(s)
(512) 338-6320
(512) 338-6301 (fax)

PTO/SB/44 (-96)
Approved for use through 6/30/99. OMB 0651-0033
Patent and trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO : 6,826,586
DATED : November 30, 2004
INVENTOR(S) : Sheueling Chang

It is certified that error(s) appear(s) in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 5, line 62, "k = (1 00 ... 0 111 0 ... 0 101 0 ... 00 1101)" should read -- k = (1 00 ... .. 0 111 0 ... ... 0 101 0 ... ... 00 1101) -- .

Claim 13, column 10, line 12, "doubling" should read -- doublings -- .

Claim 17, column 10, line 21, following "wherein the" delete "$y_n$is" and replace with -- y_n is -- .

Claim 17, column 10, line 22, following "with" delete "y_n 32 x_{n-1}^2 "and replace with – "$y_n = x_{n-1}^2$-- .

Claim 17, column 10, line 22, following "slope$_n$" delete "30" and replace with -- + -- .

MAILING ADDRESS OF SENDER:
ZAGORIN O'BRIEN GRAHAM LLP
7600B N. Capital of Texas Hwy., Suite 350
Austin, Texas 78731

PATENT NO. 6,826,586

FEB 1 5 2005